GUIA COMPLETO
SCAN DE REDES COM NMAP
TÉCNICAS BÁSICAS E AVANÇADAS DE ENUMERAÇÃO E DESCOBERTA DE SERVIÇOS OCULTOS
FUNDAMENTOS E CONCEITOS DO NMAP
SCANS BÁSICOS E AVANÇADOS
ENUMERAÇÃO DE SERVIÇOS E PROTOCOLOS
DESCOBERTA DE SERVIÇOS OCULTOS
SCRIPTS NSE E AUTOMAÇÃO
SALVAMENTO E ANÁLISE DE RESULTADOS
PARA USO EM AMBIENTES AUTORIZADOS E LABORATÓRIOS DE TESTES
LABORATÓRIO PRÁTICO PASSO A PASSO
EXEMPLOS REAIS E SIMULAÇÕES
BOAS PRÁTICAS E ÉTICA
NMAP

Guia Prático de Nmap

Técnicas Básicas e Enumeração Avançada de Redes

Aviso Importante

Utilize o Nmap apenas em ambientes autorizados, laboratórios próprios, CTFs ou redes onde você possui permissão explícita para testes. O uso indevido pode violar políticas de segurança e legislação local.

Introdução

O Nmap (Network Mapper) é uma das ferramentas mais utilizadas para descoberta de hosts, análise de portas, identificação de serviços e auditoria de redes.

Com ele é possível:

- Descobrir dispositivos ativos
- Identificar portas abertas
- Detectar serviços e versões
- Descobrir sistemas operacionais
- Enumerar serviços de rede
- Automatizar auditorias básicas

Instalação do Nmap

Debian/Ubuntu

sudo apt update

sudo apt install nmap -y

Fedora

sudo dnf install nmap

Arch Linux

sudo pacman -S nmap

Windows

Baixe pelo site oficial:

https://nmap.org

Conceitos Fundamentais

O que é uma porta?

Portas são canais de comunicação utilizados pelos serviços de rede.

Exemplos comuns:

Porta	Serviço
22	SSH
80	HTTP
443	HTTPS
3306	MySQL
3389	RDP

Descoberta Básica de Hosts

Verificar hosts ativos

nmap -sn 192.168.0.0/24

Explicação

- -sn → Apenas descoberta de hosts
- /24 → Varredura da rede inteira

Resultado esperado:

Nmap scan report for 192.168.0.1

Host is up

Nmap scan report for 192.168.0.10

Host is up

Scan Básico de Portas

Escaneando um host

nmap 192.168.0.10

O Nmap irá verificar as portas mais comuns.

Scan Completo de Portas

Verificar todas as 65535 portas

nmap -p- 192.168.0.10

Explicação

- -p- → Escaneia todas as portas TCP

Descoberta de Serviços

Detectando versões

nmap -sV 192.168.0.10

Exemplo de saída

22/tcp open ssh   OpenSSH 8.4

80/tcp open http   Apache 2.4.54

3306/tcp open mysql MariaDB

Identificação de Sistema Operacional

sudo nmap -O 192.168.0.10

Explicação

- -O → Detecção de sistema operacional

Técnicas de Enumeração

Enumeração é o processo de coletar informações detalhadas sobre serviços ativos.

Enumeração HTTP

Descoberta de títulos de páginas

nmap --script http-title 192.168.0.10

Descoberta de headers HTTP

nmap --script http-headers 192.168.0.10

Descoberta de métodos HTTP

nmap --script http-methods 192.168.0.10

Enumeração SMB

nmap --script smb-os-discovery 192.168.0.10

Possíveis informações:

- Nome da máquina
- Sistema operacional
- Domínio
- Compartilhamentos

Enumeração DNS

nmap --script dns-brute exemplo.local

Pode ajudar a identificar:

- Subdomínios
- Hosts internos
- Serviços escondidos

Descoberta de Serviços Ocultos

Serviços ocultos normalmente utilizam:

- Portas não padrão
- Serviços internos
- Aplicações esquecidas
- Ambientes de teste

Estratégias de Descoberta

1. Scan completo de portas

nmap -p- -T4 192.168.0.10

2. Descoberta de serviços e versões

nmap -sV -p- 192.168.0.10

3. Scan UDP básico

sudo nmap -sU 192.168.0.10

Serviços UDP frequentemente ignorados:

- DNS
- SNMP
- NTP
- TFTP

Técnicas Avançadas de Enumeração

NSE — Nmap Scripting Engine

O NSE permite automatizar verificações e auditorias.

Listando scripts disponíveis

ls /usr/share/nmap/scripts/

Executando múltiplos scripts

nmap --script vuln 192.168.0.10

Observação

Esse tipo de script deve ser utilizado somente em laboratórios autorizados.

Enumeração SSL/TLS

nmap --script ssl-cert,ssl-enum-ciphers -p 443 192.168.0.10

Permite:

- Identificar certificados
- Detectar protocolos antigos
- Avaliar cifras disponíveis

Enumeração SNMP

nmap -sU -p 161 --script snmp-info 192.168.0.10

SNMP pode revelar:

- Nome do host
- Informações do sistema
- Equipamentos de rede

Técnicas de Timing

Ajustando velocidade do scan

nmap -T4 192.168.0.10

Perfil	Velocidade
T0	Muito lento
T1	Lento
T2	Moderado
T3	Padrão
T4	Rápido
T5	Muito agressivo

Salvando Resultados

Salvar em TXT

nmap -oN resultado.txt 192.168.0.10

Salvar em XML

nmap -oX resultado.xml 192.168.0.10

Simulação de Cenário

Objetivo

Descobrir serviços ativos em um servidor de laboratório.

Etapa 1 — Descoberta do host

nmap -sn 192.168.1.0/24

Host encontrado:

192.168.1.15

Etapa 2 — Descoberta de portas

nmap -p- 192.168.1.15

Resultado:

22/tcp open ssh

80/tcp open http

8080/tcp open http-proxy

3306/tcp open mysql

Etapa 3 — Descoberta de versões

nmap -sV 192.168.1.15

Resultado:

Apache 2.4.54

MariaDB 10.5

OpenSSH 8.4

Etapa 4 — Enumeração HTTP

nmap --script http-title,http-headers 192.168.1.15

Possível descoberta:

Painel administrativo interno

Servidor Apache Ubuntu

Boas Práticas

- Sempre tenha autorização formal
- Evite scans agressivos em produção
- Documente resultados

- Utilize ambientes de laboratório
- Atualize regularmente o Nmap

Ambientes Recomendados para Treino

- Máquinas virtuais locais
- Laboratórios CTF
- Redes internas autorizadas
- Containers Docker

Comandos Úteis

Objetivo	Comando
Descobrir hosts	nmap -sn rede/24
Scan rápido	nmap host
Todas as portas	nmap -p- host
Detectar versões	nmap -sV host
Detectar SO	nmap -O host
Scripts NSE	nmap --script nome host
Scan UDP	nmap -sU host

Conclusão

O Nmap é uma ferramenta extremamente poderosa para auditoria e administração de redes. Dominar técnicas básicas e avançadas de enumeração ajuda profissionais de segurança e administradores a compreender melhor a superfície de exposição dos serviços.

A prática constante em ambientes controlados é fundamental para desenvolver experiência sem comprometer a segurança de terceiros.